Autor HANS-JOACHIM WINKLER

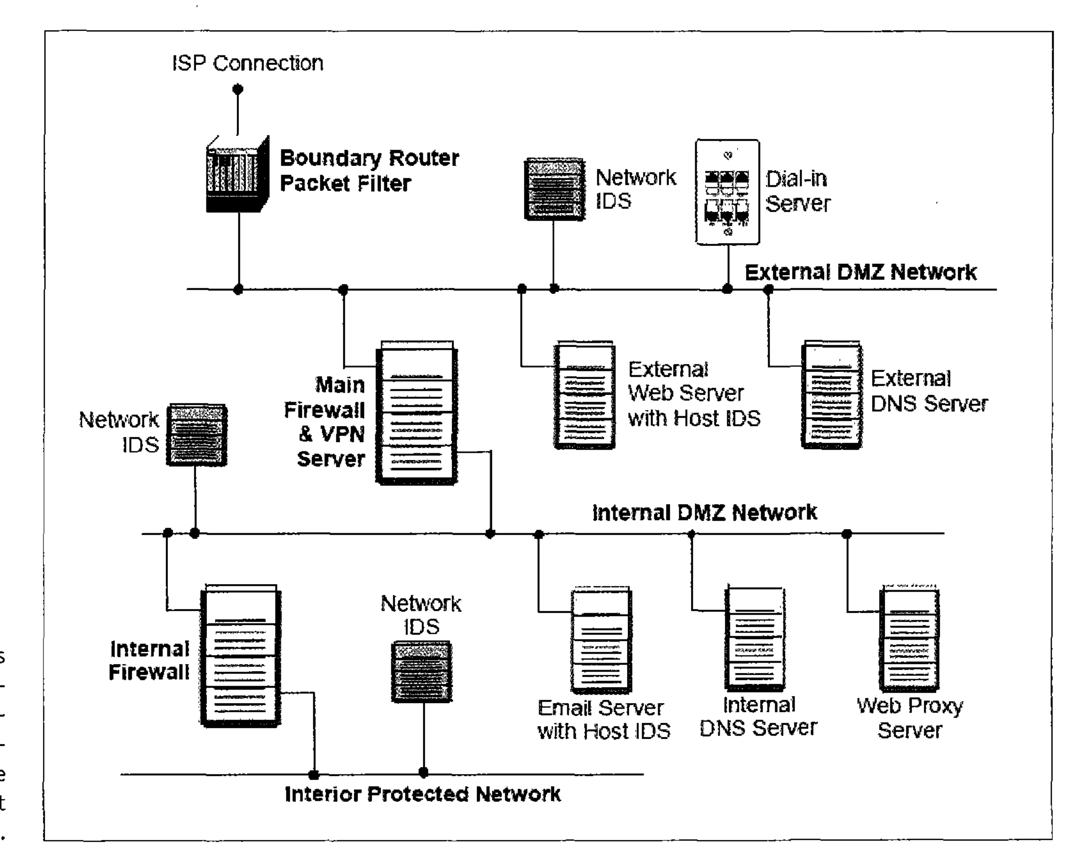
Sichere Firmen-Netzwerke

Viele Administratoren sind sich nicht bewusst, welche Angriffsziele ihr Netzwerk Hackern und Spionen bietet. Daher sollte jedes Netzwerk regelmäßig auf Schwachstellen untersucht werden. Die richtigen Tools sparen dabei den Gang zum Security-Dienstleister.

Vernetzte Rechner sind permanent Bedrohungen ausgesetzt: Im Internet finden sich Programme, die quasi auf Knopfdruck entfernte Rechner auf Schwachstellen untersuchen und sich dann oftmals auch gleich in das System einloggen. Das kann für Administratoren unangenehme Folgen haben: Spionage, Datendiebstahl oder Vernichtung der Daten können eine Firma an den Rand des Ruins bringen.
Bei der Suche nach internen Sicherheitslücken kommen im Grunde die gleichen Tools zum Einsatz, die auch ein echter Eindringling verwenden würde. Keinesfalls dürfen die im Folgenden beschriebenen Methoden auf fremde Hosts im Internet angewandt werden, da sie als Angriff oder Vorbereitung eines Angriffs gewertet werden und illegal sind.

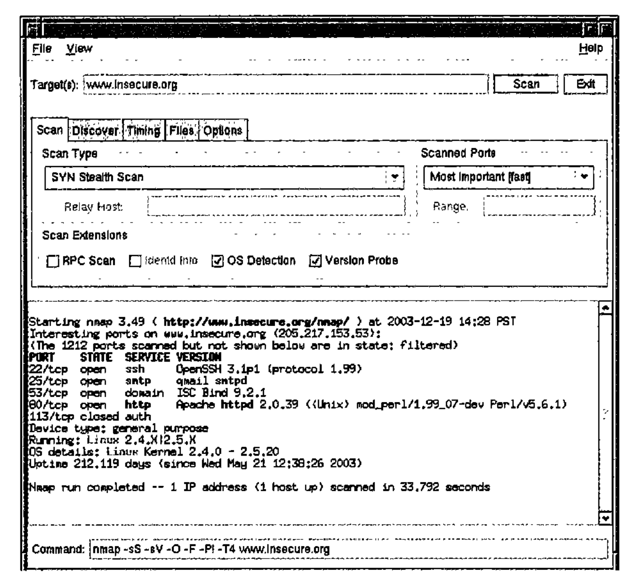
PORTSCANNER

Am Anfang einer Netzwerk-Analyse wird, wie auch am Anfang eines realen Angriffs, immer bestimmt, welche Rechner und Geräte überhaupt in einem Netzwerk vorhanden sind. Geeignet dafür sind Portscanner. Diese analysieren ein Netzwerk auf vorhandene Geräte wie Hosts, Router und Switches und ermitteln die laufenden Dienste eines Hosts wie FTP oder HTTP. Meistens finden sie auch die Anwendungen, die diese Dienste bereitstellen. Admind stellen so recht einfach fest, ob fremde Hosts oder zusätzliche und verwundbare Dienste vorhanden sind.



Die kritischen Punkte eines Netzwerks stellen die externen und die internen Firewalls sowie die Anwendungs-Server dar. Jede Sicherheitsanalyse beginnt bei diesen Geräten.

Portscanner wie Nmap *(www.insecure.org)* verwenden zuerst Ping-Sweeps, um die Anwesenheit von Hosts in einem Netzwerk zu bestimmen. Erhält der Scanner eine Antwort, wird die betreffende IP-Adresse meist für spätere Untersuchungen gespeichert. Nach der Feststellung der Anwesenheit werden TCP- und UDP-Scans durchgeführt, um die laufenden Dienste zu bestimmen. Dabei sind UDP-Scans recht unzuverlässig, da sie nicht erkennen lassen, ob ein Host beim Ausbleiben einer Antwort nicht vorhanden ist oder eine Firewall die Pakete verworfen hat. Beim einfachen TCP-SYN-Scan wird versucht, eine vollständige Verbindung zum gewünschten Port des Ziel-Hosts aufzubauen. Gelingt dies, ist damit das Vorhandensein des Dienstes bewiesen – der Port ist offen. Auf einem geschlossenen Port lauscht kein Dienst. Bei Dienst-Anfragen sendet ein geschlossener Port eine negative Antwort. Dieses RFC-konforme Verhalten wird allerdings oft zur Erhöhung der Sicherheit geändert, so dass ein geschlossener Port keine Antwort sendet. Bei blockierten Ports wird die Anfrage einfach verworfen. Dieses Verhalten deutet auf das Vorhandensein einer vorgeschalteten Firewall hin.



Nmap scannt unter Windows und Linux: Verschiedene Frontends erleichtern den Umgang mit dem Kommandozeilen-Tool.

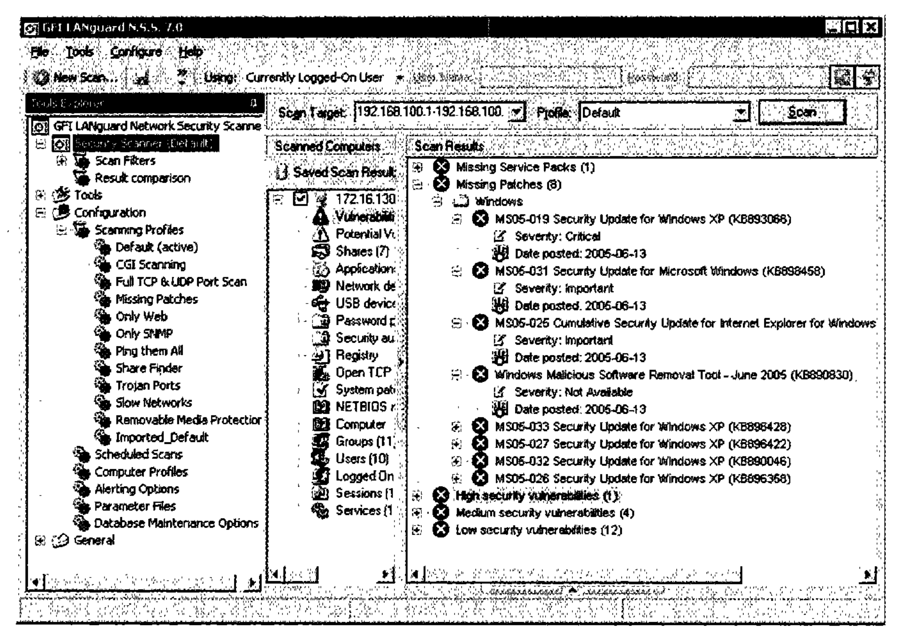
Kommt eine Verbindung zustande, senden die meisten Dienste Informationen über sich selbst an das anfragende System. So gelangen Name der Server-Anwendung, Versionsnummer und weitere Informationen auf ein fremdes System. Mit diesen Informationen kann ein Angreifer nach Lücken in der eingesetzten Server-Software suchen.

GUTE UND BÖSE SCANS

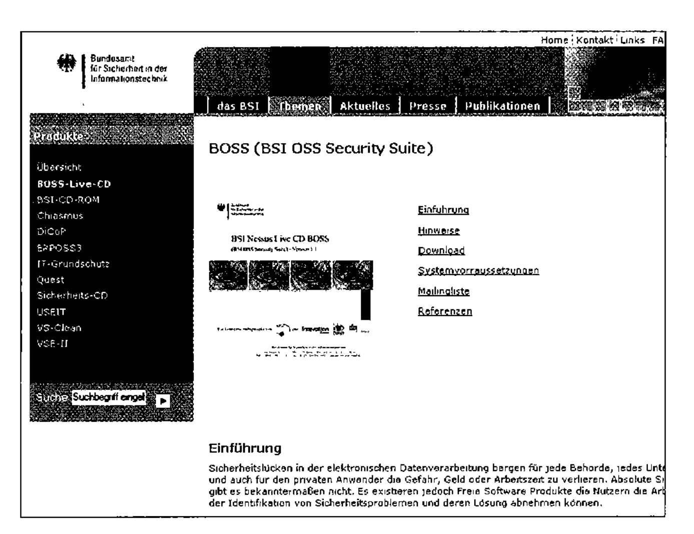
Es gibt eine Fülle verschiedener Port-Scans, die versuchen, dem gescannten System mit allerlei Tricks Informationen zu entlocken, wobei bestimmte Eigenschaften des TCP genutzt werden. Ein Standard-Scan ist zum Beispiel der TCP-Half-open-Scan: Wichtig für einen Angreifer ist es, unentdeckt zu bleiben, da Port-Scans geloggt werden und dadurch Hinweise auf eventuell bevorstehende Angriffe geben. So kann sich das scannende System etwa über halb offene Verbindungen verstecken. Bei halb offenen Verbindungen wird ein SYN an das Zielsystem gesendet, das seinerseits mit einem ACK antwortet. Danach muss das anfragende System mit einem weiteren ACK den Verbindungswunsch bestätigen – damit ist die Verbindung aufgebaut (Drei-Wege-Handshake). Bleibt das zweite ACK aus, liegt eine halb offene Verbindung vor. Da in solchen Fällen keine vollständige TCP-Verbindung zustande kommt, erfolgt auch kein Eintrag in der Log-Datei. Half-open-Scans werden als Vorbereitung eines Angriffs gewertet. Sie belästigen das Zielsystem, das für jede Verbindung Arbeitsspeicher bis zum Time-out belegt. Die Dokumentationen der Scanner enthalten weiterführende Erklärungen zu den Scan-Arten.

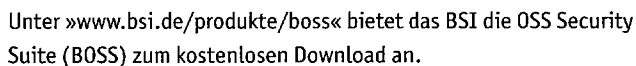
OS-FINGERPRINTING

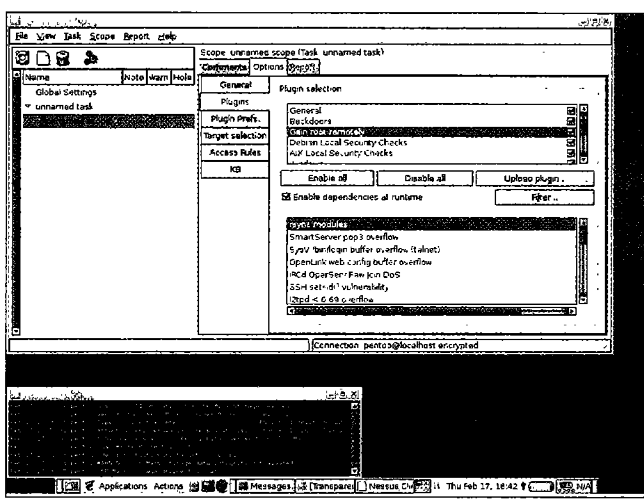
Gut ausgestattete Scanner versuchen mit unterschiedlichen Methoden, den Typ des Betriebssystems in Erfahrung zu bringen. Für dieses OS-Fingerprinting wertet der Scanner verschiedene



Gfi LANGuard ist ein komplexer Scanner und eignet sich besonders für Windows-Umgebungen: Nach einem Scan auf ein entferntes System werden beispielsweise fehlende Patches für Windows und den Internet Explorer bemängelt.




Unter »www.bsi.de/produkte/boss« bietet das BSI die OSS Security Suite (BOSS) zum kostenlosen Download an.



Security-Scanner wie Nessus arbeiten mit umfangreichen Datenbanken, die täglich aktualisiert werden.

Informationen aus: Offene NetBIOS-Ports deuten beispielsweise auf Windows-Rechner hin. Auch aus der Art, wie die TCP-Sequenznummern gebildet werden, lassen sich Rückschlüsse ziehen. TTL-Werte sind ebenfalls typisch für Betriebssysteme. Alle diese Informationen sind aber nur Hinweise, keinesfalls erlauben sie das sichere Erkennen eines bestimmten Betriebssystems. Administratoren können diese Werte nämlich verändern und damit die Scanner täuschen. Die Ergebnisse der Port-Scans lassen sich in Datenbanken speichern. Durch einen Abgleich mit bereits erfolgten Scans lassen sich neue Hosts sowie unerwünschte und verwundbare Dienste erkennen.

ERGEBNISSE AUSWERTEN

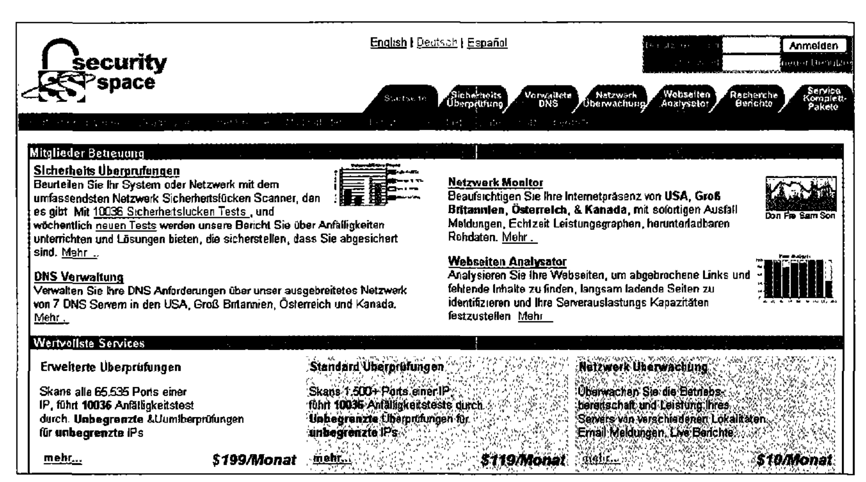
Portscanner arbeiten weitgehend automatisch, die Interpretation der Ergebnisse obliegt aber dem Administrator. Zur Auswertung sollte er regelmäßig Webseiten mit Sicherheitshinweisen besuchen, zum Beispiel DFN-CERT *(www.dfn-cert.de)*, ISC *(www.isc.org)*, SANS *(www.sans.org)* und Microsoft *(www.microsoft.com/security)*. Hilfreich ist es, sich auf entsprechende Mailinglisten setzen zu lassen. Eine gute Anlaufstelle ist zudem die Webseite www.sicher-im-netz.de. Für die Initiative »Deutschland sicher im Netz« engagieren sich beispielsweise Mcert Deutsche Gesellschaft für IT-Sicherheit, die Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (fsm) und der TeleTrusT Verband sowie die Firmen Computer Associates, eBay, Microsoft, MSN, SAP und T-Online. Gemeinsames Ziel: Mit dem IT-Sicherheitspaket Mittelstand sollen Unternehmen von der Notwendigkeit geeigneter Sicherheitsmaßnahmen überzeugt und zugleich bei deren Umsetzung unterstützt werden. Auf der kostenlosen CD finden Sie dazu Sicherheitsrichtlinien, Verfahrensanweisungen, Checklisten und Notfallpläne sowie einige Tools.

VULNERABILITY-SCANNER

Bei der Auswertung ebenfalls sehr hilfreich sind die Vulnerability-Scanner. Als Weiterentwicklung der Portscanner nutzen Vulnerability-Scanner Datenbanken mit bekannten Schwachstellen von Server-Software und Betriebssystemen. So können die Programme spezifische Warnungen und Hinweise zur Schließung der Lücken geben. Sie sind beim Aufspüren veralteter Software hilfreich und entdecken automatisch, ob auf den gescannten Systemen bestimmte Patches oder Service-Packs installiert sind. Einige Scanner bieten auch gleich das Verteilen und Installieren von Patches und Service-Packs an – Administrator-Rechte auf den Zielsystemen sind dabei Voraussetzung. Unterschieden werden Netzwerk- und Host-basierte Scanner. Letztere erfordern Administrator-Rechte auf den Hosts und liefern mehr Details über Schwachstellen – teilweise reparieren sie diese sogar. Netzwerk-basierte Scanner sind dagegen unabhängig von Betriebssystemen. Sie liefern weniger Details, sind dafür aber schneller. Vulnerability-Scanner listen zwar erkannte Schwachstellen auf, können aber keine Zusammenhänge zwischen diesen erkennen. Mehrere als harmlos eingestufte Sicherheitslücken können in ihrer Kombination ein folgenschweres Sicherheitsloch aufreißen. Hier ist das Wissen des Administrators gefordert. Zu den weiteren Nachteilen dieser Scanner gehört ein erhöhter Netzwerk-Verkehr, da relativ viele Informationen übertragen werden müssen. Und die Datenbank muss ständig aktuell gehalten werden. Je schneller diese auf den aktuellen Stand gebracht wird, desto besser ist das Produkt. Schwachstellenprüfungen sollten viertel- bis halbjährlich durchgeführt werden, auf besonders exponierten Maschinen mit direkter Internet-Anbindung wie Web-Server sollten sie laufend erfolgen.

PASSWORT-CRACKING

Passwörter – besonders die von Administratoren – sind ein beliebter Angriffspunkt in Netzwerken und auf lokalen Maschinen. Die Wahl eines guten Passworts kann ein Cracken zwar nicht verhindern, aber erschweren. Gute Pass-



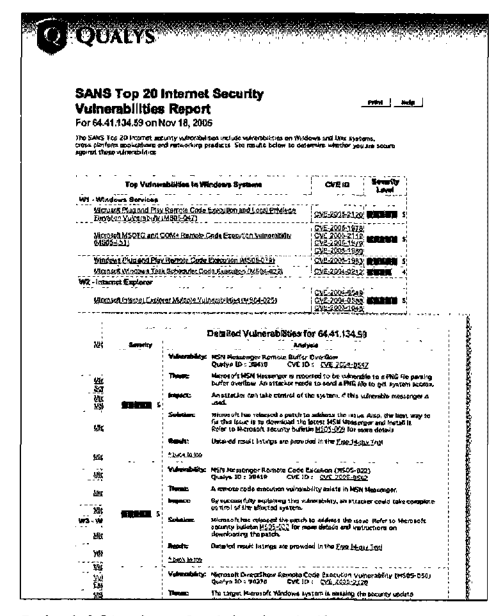
Bei Securityspace.com können Sie die Überwachung des Netzwerks in fremde Hände legen. Im Angebot sind zahlreiche Netzwerk-Sicherheits-Überprüfungs-Dienste.

wörter sind mindestens acht Zeichen lang und bestehen aus kleinen und großen Buchstaben sowie aus Ziffern und Sonderzeichen. Über Passwortrichtlinien können zum Beispiel in Windows-Domänen Komplexität, Verfallsdatum, Zeitfenster, Historie und anderes erzwungen werden – ein Angriffspunkt bleiben sie aber dennoch. Administratoren nutzen Passwort-Cracker, um die Passwörter der Anwender auf Schwächen hin zu untersuchen – nicht selten sind Passwörter in Sekundenschnelle geknackt. Die gleichen Tools nutzen aber auch Hacker.
Passwörter können entweder im Segment mit einem Sniffer gelesen oder durch lokalen Zugang zu einer Maschine in Erfahrung gebracht werden, wobei aber in der Regel Administrator-Rechte nötig sind. Das Sniffen im Netzwerk funktioniert nur innerhalb eines Segmentes oder durch Cache-Poisoning. Für das Auslesen zum Beispiel aus einer Windows-Installation spielt man üblicherweise ein zweites Betriebssystem auf wie Linux und bearbeitet die Registrierung. Ein bekanntes Programm ist L0phtcrack. Solche Passwort-Cracker arbeiten mit (modifizierten) Wörterbuch-Attacken, die lange Wörterlisten benutzen und mit dem bekannten, aber verschlüsselten Passwort vergleichen, genauer gesagt, werden Hashes verglichen. Jedes Passwort, das in einem Wörterbuch vorkommt, ist deswegen ein schwaches Passwort.

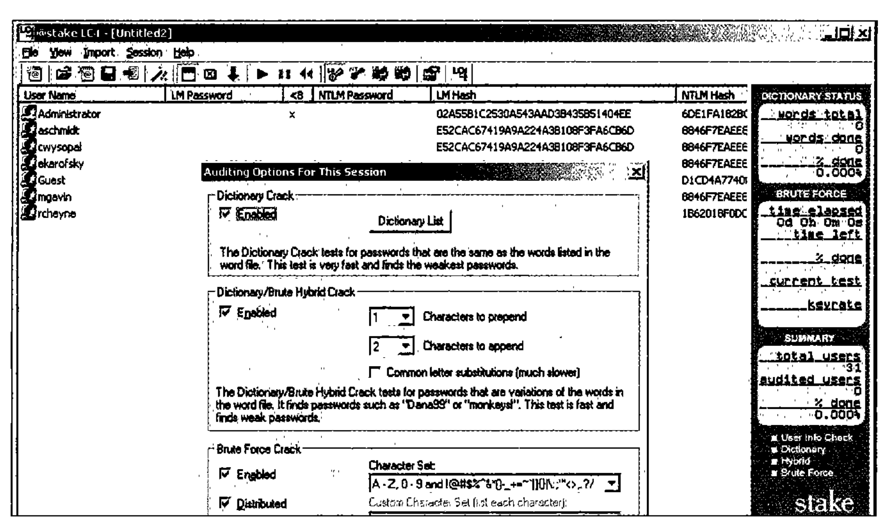
Modifizierte Wörterbuch-Attacken ändern Wörter durch Austausch von Buchstaben durch Ziffern oder durch Zufügen von ZIffern und Ähnlichem. Wird das Passwort damit nicht gefunden, wird eine Brute-Force-Attacke gestartet, die immer zum Ziel führt – genügend Zeit und Rechenleistung vorausgesetzt. Ein beliebtes Angriffsziel ist auch die Rettungsdiskette von Windows, die das Passwort enthält. Passwort-Cracking ist eine Routineaufgabe bei Penetration-Tests.

PENETRATION-TESTING

Die Sicherheit von Netzwerken kann mit Penetration-Tests geprüft werden. Dabei versucht man, unter Umgehung der bestehenden Sicherheitsmaßnahmen Zugriff auf die Ziel-Systeme zu erlangen. Solche Tests können innerhalb eines Netzwerks oder von außerhalb durchgeführt werden. Zum Einsatz kommen dabei Tools und Techniken, die auch echte Angreifer verwenden. Bevor solche simulierten Angriffe durchgeführt werden, ist eine Absprache mit dem Management und den Administratoren notwendig. Dazu gehört mindestens, welche Systeme mit welchen Mitteln wann untersucht werden. Neben der zusätzlichen Belastung des Netzwerks besteht bei solchen Tests auch die Möglichkeit der Beschädigung der Ziel-Hosts. Ein externer Angriff auf einen bekannten IP-Bereich beginnt mit Scannern. Weitere Informationen liefern DNS- und Whois-Abfragen sowie möglicherweise die Web- und LDAP-Server einer Firma. Bei der Beschaffung von Informationen sind echte Angreifer sehr erfindungsreich: So sind angebliche Mails der IT-Administration, die zur Herausgabe eines Passworts auffordern, genauso üblich wie telefonische Anfragen bei Mitarbeitern (Social Engineering). Auch durch Spyware-Komponenten können weitere Informationen beschafft werden.
Da externe Angreifer in der Regel durch Firewalls hindurch müssen, kommen als Transport-Möglichkeit nur die erlaubten Protokolle, meistens FTP, HTTP, SMTP und POP3, in Frage. Haben die Tester Zugriff auf einen internen Host erlangt, wird versucht, von dort aus weitere Hosts zu kompromittieren, die von außen nicht sichtbar sind. Bei Angriffen von innen gibt es weitere Möglichkeiten der Informationsbeschaffung: Sniffing und NetBIOS-Scans liefern mitunter detaillierte Daten über Netzwerke und Hosts, manchmal sogar Passwörter. Sind alle Ziel-Hosts bekannt und ihre Schwachstellen mit Scannern entdeckt, erfolgen die eigentlichen Angriffe. Viele Attacken sind im Internet dokumentiert und Bestandteil der Scanner-Datenbanken.



Beispiel für einen Bericht des Online-Scanners von Qualys: Neben Erklärungen zu den gefundenen Sicherheitslücken gibt es Tipps und Anleitungen.



Bei Brute-Force-Attacken wird versucht, durch simples Ausprobieren verschiedener Passwortmöglichkeiten aus einem Wörterbuch Zugang zum System zu erlangen.

Solche Lücken lassen sich meist schnell durch Einspielen von Patches schließen. Andere Angriffe sind neu, manche sogar äußerst kreativ – Entdeckung und Rückverfolgung können dann schwierig und zeitintensiv sein.
Die meisten Schwachstellen beruhen auf Lücken im Kernel sowie den Server-Programmen. Gelingt es, den Kernel zu kompromittieren, kann das System meistens beliebig manipuliert werden. Architekturen wie Windows (aber teilweise auch Unix/Linux) lassen sich mit etwas Geschick völlig zum Zusammenbruch bringen, da sie per Design nicht auf Sicherheit getrimmt sind. Jedes laufende Programm, das durch Spyware oder Trojanische Pferde eingeschleppt wurde, kann jedes Windows-System vollständig aushebeln und die Kontrolle einem Angreifer übertragen.
Penetration-Tests beweisen die Existenz von Sicherheitslücken. Am Ende steht ein Bericht der gefundenen Schwachstellen, der eine Risikoabschätzung ermöglicht sowie Hinweise auf die Beseitigung der Schwachstellen enthält. Konsequenzen von Penetration-Tests können eine Anpassung der Sicherheitsrichtlinien des Unternehmens sein oder ebenso die Erkenntnis, dass Systeme falsch konfiguriert sind und Software Sicherheitslücken aufweist beziehungsweise verfügbare Patches nicht eingespielt wurden. Auch größere Änderungen in der Sicherheitsarchitektur können die Folge von Penetration-Tests sein: etwa das Einziehen einer weiteren Sicherheitsebene durch den Einsatz zusätzlicher Firewalls, ein zentrales Patch-Management oder auch einheitliche Arbeitsplatz-Umgebungen durch Cloning.

LOG-FILE-ANALYSE

Firewall- und IDS-Logs, Server-Logs sowie jede Art von Log-Dateien können Aufschluss über ein auffälliges Verhalten eines Systems geben und zwar durch Vergleich über einen längeren Zeitraum oder auch durch Anzeige des aktuellen Zustands. Unter Windows Server können etwa Zugriffe auf das Dateisystem aufgezeichnet und nicht autorisierte Zugriffe auf bestimmte Verzeichnisse gemeldet werden. IDS-Logs wie von Snort *(www.snort.org)* führen Protokollanalysen durch und erkennen Angriffsmuster wie Port-Scans, Buffer-Overflow- und SMB-Attacken oder Fingerprinting-Versuche. Filter und Sortierfunktionen erleichtern das Finden der gesuchten Informationen. Log-File-Analysen sollten regelmäßig durchgeführt werden, wichtige Server sowie Firewalls sollten täglich überprüft werden.

ANDERE SCHWACHSTELLEN

Weitere Sicherheitslücken entstehen durch Modems und Funknetze. Auch wenn Modems kaum noch verwendet werden, besteht die Möglichkeit, diese im Büro anzuschließen und damit einen nicht gesicherten Zugang zum Netzwerk zu schaffen. Modems können mit Wardialern entdeckt werden, die eine Liste mit Telefonnummern abtelefonieren. In manchen Firmen kommt auch ein zweites, unsicheres Netzwerk zum Einsatz, das häufig für Testzwecke verwendet wird. Durch Einbau einer zweiten Netzwerkkarte in einen Client kann dieser zum Router werden, wodurch die Sicherheit des Firmennetzwerks umgangen wird.
Funknetze lassen sich gut mit Scannern erkennen, die bereits im Lieferumfang der Funkkarte enthalten sind. Tools wie etwa Airsnort *(airsnort.shmoo.com)* oder WEPCrack *(www.sourceforge.net/projects/wepcrack)* zeigen, wie schnell sich WEP-Keys knacken lassen. Access-Points sollten daher möglichst mit WAP und nicht mit WEP gesichert werden.
Manchmal werden bei einem Einbruch Dateien wie das *host*-File geändert. Solche Manipulationen lassen sich mit File-Integrity-Checkern wie der Change-Auditing-Software Tripwire *(www.tripwire.com)* erkennen. Das Sicherheits-Tool legt eine Datenbank des Filesystems an, um Veränderungen und Manipulationen an Verzeichnissen und Dateien feststellen zu können. Es ist auf Linux-Basis als Open-Source-Software verfügbar, aber auch als kommerzielle Variante für Windows.

ONLINE-SCANNER

Wer sich nicht selbst mit Tools im Netzwerk beschäftigen möchte, kann die Dienste eines Online-Scanners in Anspruch nehmen. Es gibt eine ganze Reihe an Angeboten, zum Beispiel von Qualys *(www.qualys.com)* oder Securityspace *(www.securityspace.com)*, die aber kostenpflichtig, meist in Form von Abonnements, vertrieben werden. Im Repertoire sind meistens Tausende von Sicherheitstests für verschiedene Umgebungen, die online über das Internet durchgeführt werden. Die abschließenden Reports sind sehr detailliert und geben Hinweise, wie gefundene Lücken zu schließen sind. ■